Space Network (SN)

Web Services Interface (SWSI)

Server Training

June 23-27, 2003

Agenda

- **System Overview**
- **Client Software Operation & Demo**
- **Server Configuration**
- **Server Operation**
- **Customer and User Setup**
- **Database Design and Management**
- **Database Administration**
- **Digital Certificate Management**
- **System Administration Procedures**
- **Problem Reporting and Tracking**
- **Troubleshooting Procedures**

Section 1
System Overview

Capabilities
Client Requirements
SWSI Architecture
Hardware Components
Software Components

Capabilities

- **Standards-based customer interface for performing TDRS scheduling, real-time service monitoring and control**
- **Primary customer interface for Demand Access System (DAS) scheduling, service monitoring & control Multi-mission support**
- **Accessible from the Internet and NISN Open & Closed IONet**
- **Secure access through encryption, certification, and authentication**
- **Cross-platform compatible client application (Windows, Unix, etc.)**
- **Java-based Graphical User Interface (GUI)**
- **Supports full NCCDS/Mission Operations Center (MOC) interface**

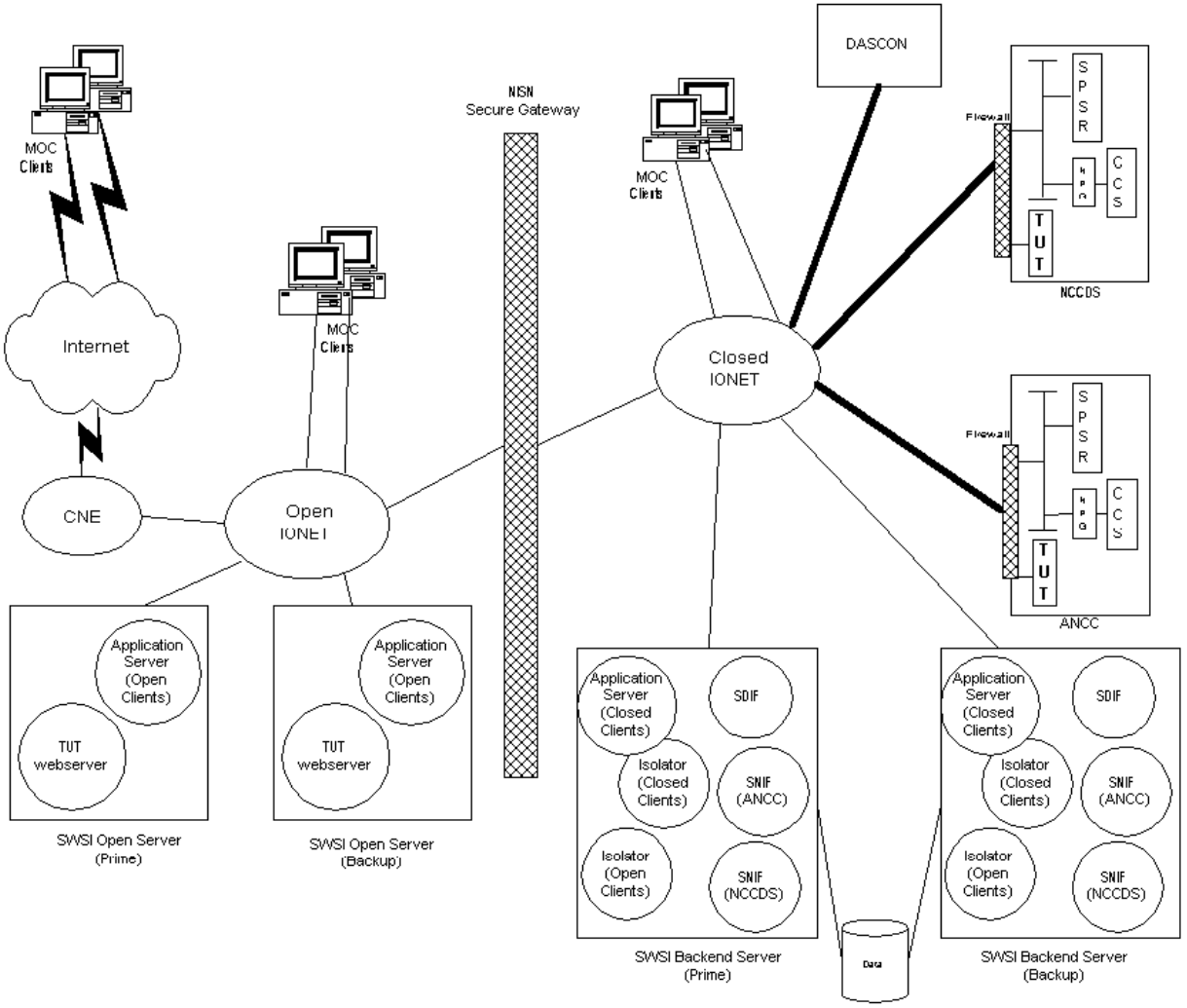
Capabilities (Cont'd)

- **Orbiting or stationary state vector generation based on user input of geocentric (position & velocity) or geodetic (latitude, longitude, & altitude) coordinates**
- **Internet and Open IONet access to TDRSS Unscheduled Time (TUT)**
- **Test mode for performing Engineering Interface (EIF) testing and user training**
- **Initial Release 03.1 supports only NCCDS interface. DAS interface will be provided in Release 03.2 by October, 2003.**

Client Requirements

- **Sun Microsystems Java Runtime Environment (JRE) 1.4.1 (free)**
- **Tested Operating Systems: Windows 98/NT/2000; Solaris 7,8; Linux**
- **128 MB RAM**
- **2 MB Disk Space (application size, excluding logs)**
- **1024x768 16 bit color display**
- **Web browser to view TUT**

SWSI Architecture



Hardware Components

- **Client Workstation**
  - User's desktop workstation
  - Supports JRE 1.4.1
- **Backend Server**
  - Hosts most of SWSI server applications
  - Manages user login sessions, database storage, and communications with NCCDS, ANCC, and DAS
- **Open Server**
  - Proxy server to allow Open IONet and Internet-based users to connect to SWSI and access TUT
  - User requests directed to Backend Server through NISN Secure Gateway

Software Components

- **Client**
  - Executes on Client workstation
  - Provides Graphical User Interface (GUI) for performing SWSI client operations
- **Application Server**
  - Server process that Client connects to for accessing SWSI services
  - Tracks user requests and provides responses to the Client
  - Separate instances run on Open and Backend Servers
- **Isolator**
  - Server process provides interface for Client with SWSI Database
  - Processes users requests and generates responses
  - Communicates with Client through Application Server
  - Separate Isolator required for each Application Server

Software Components (Cont'd)

- **SWSI-NCCDS Interface (SNIF)**
  - Server process that communicates with NCCDS using NCCDS/MOC messaging protocol
  - Separate SNIF required for each NCC (operations NCC and ANCC)
- **SWSI-DAS Interface (SDIF)**
  - Server process that communicates with DAS using DAS/SWSI messaging protocol
  - Separate SDIF required for each DAS (operations DAS and HMD test bed)
  - Not provided in initial SWSI release
- **Database**
  - Backend data storage for customer configuration and scheduling data
- **Open TUT Server**
  - Web server mirrors TUT services provided by NCCDS on Closed IONet
  - TUT data updated hourly

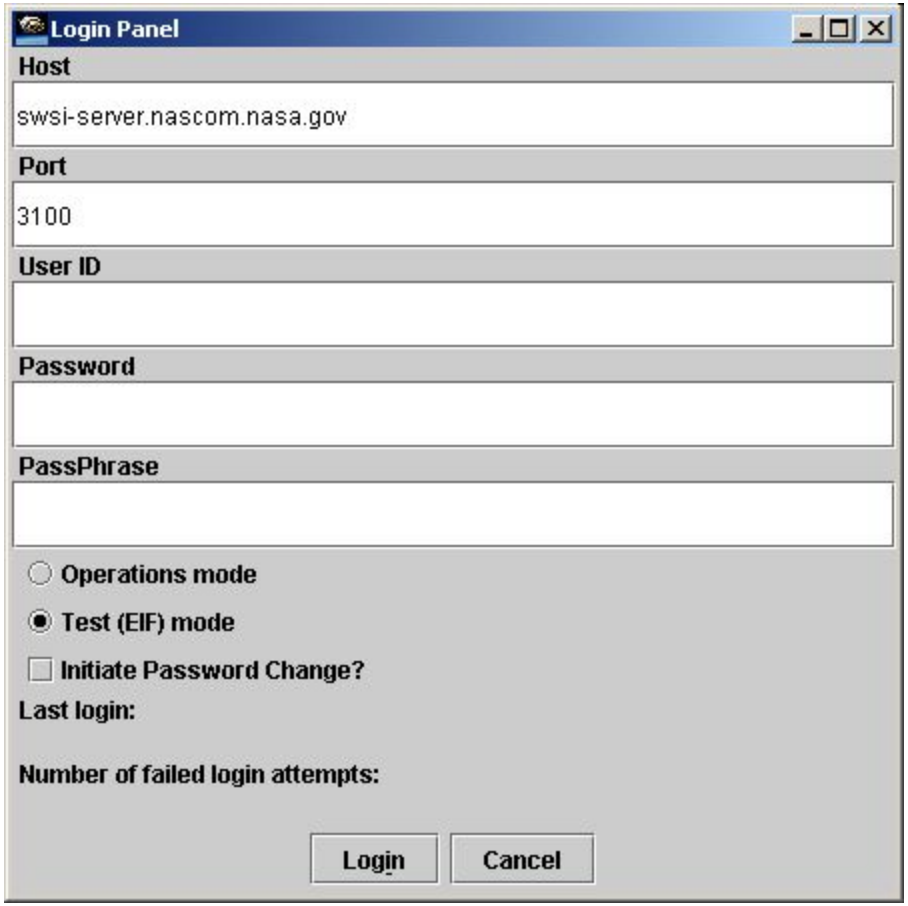
Section 2
Client Software Operation

Installation & Setup
Client Operation

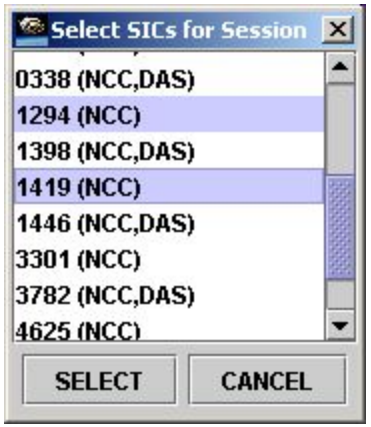
Installation & Setup

- **Client workstation software requirements**
  - JRE 1.4.1 to run Client application
  - Web browser (Netscape, Internet Explorer, Mozilla, Opera, etc) to view TUT and download SWSI Client software and digital certificates
  - System Clock synchronized to network time source
- **Rules of Behavior must be read and signed**
- **IP address(es) must be provided to SWSI DBA or SysAdmin to grant access to SWSI Servers for software download and Client connection**
- **Access SWSI Server to generate certificate and download Client software. JRE software also provided on servers.**
  - Closed IONet address https://swsi-server.ops.nascom.nasa.gov/
  - Open IONet address https://swsi-server.nascom.nasa.gov/
- **Detailed installation instructions provided on server and with Client software download.**

Login


Login Panel
Host
swsi-server.nascom.nasa.gov
Port
3100
User ID
Password
PassPhrase
Operations mode
Test (EIF) mode
Initiate Password Change?
Last login:
Number of failed login attempts:
Login
Cancel

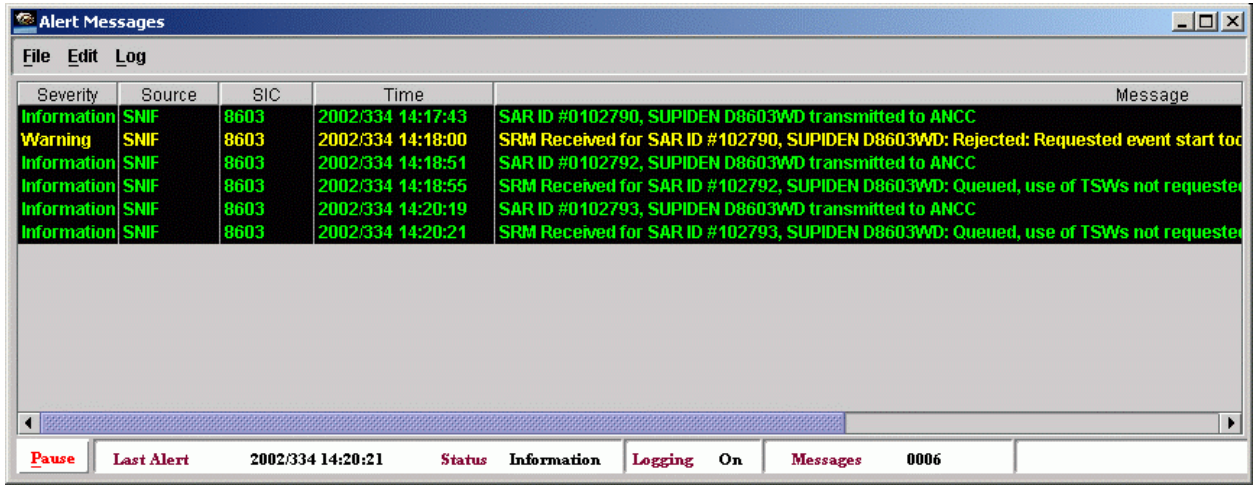
SIC Selection



Main Control Panel

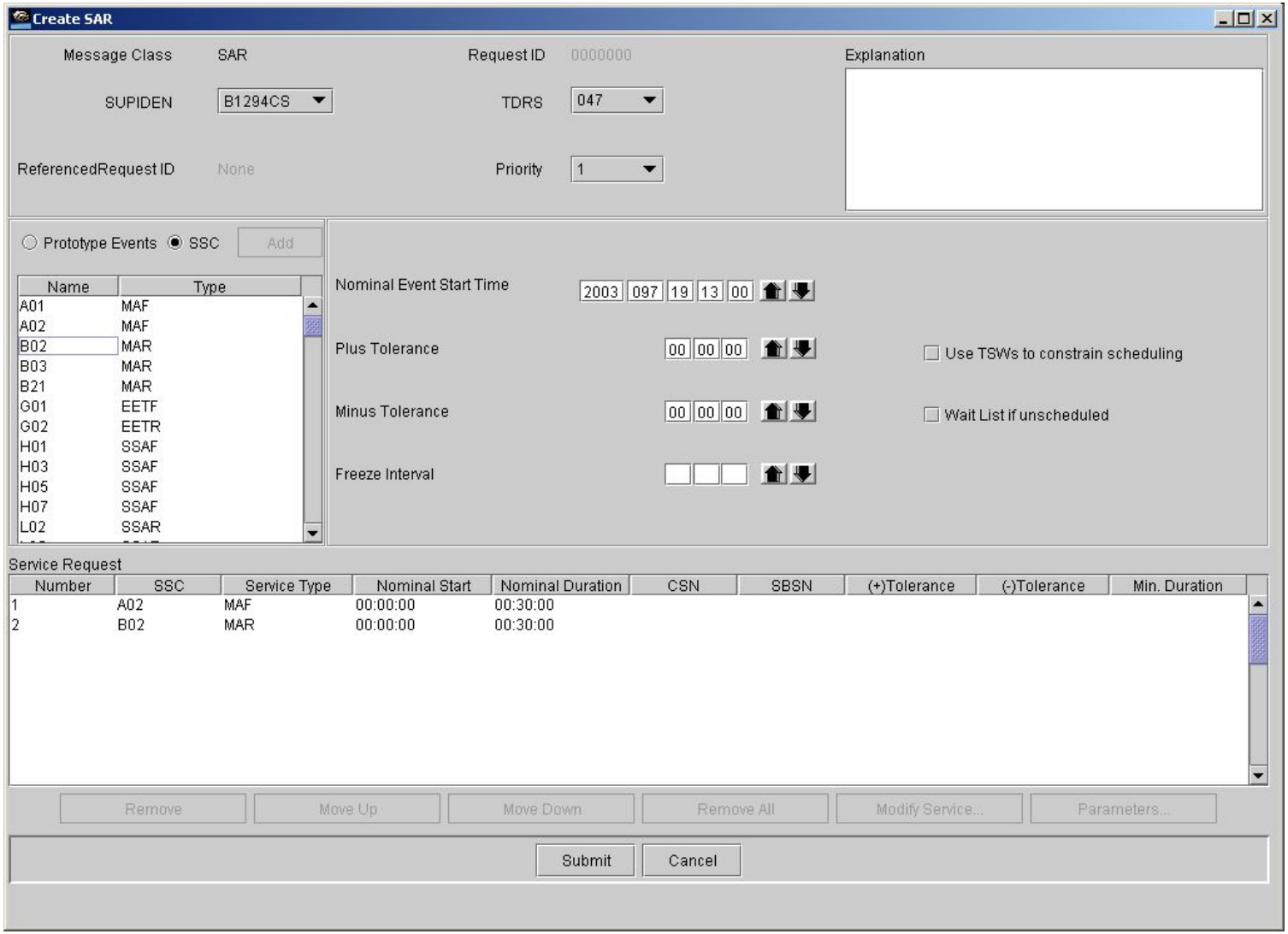
- **Process status useful for troubleshooting server problems**

Alert Message Panel

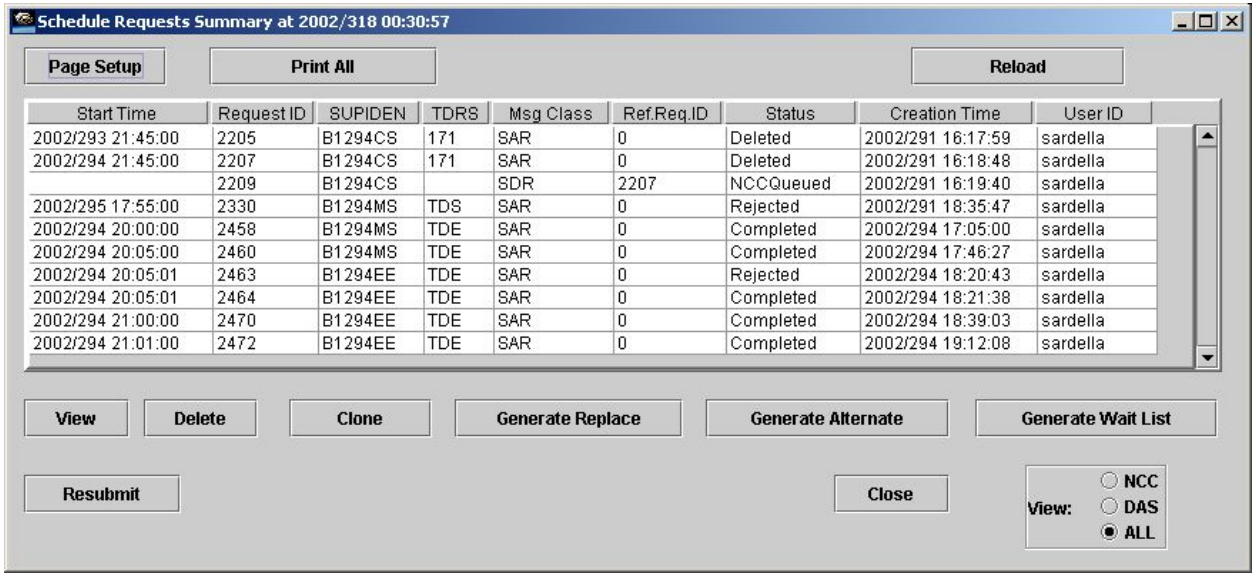


- **Alert Severity**
  - Information (green) – successful processing with additional information
  - Warning (yellow) - successful processing by SWSI, but with warning information, such as request rejected by NCCDS
  - Critical (red) – SWSI software, system, or Database problem. Requires resolution by SWSI operator, SysAdmin, or developer
- **Source**
  - Client, ISO, SNIF, SDIF, or DAS

Creating a SAR

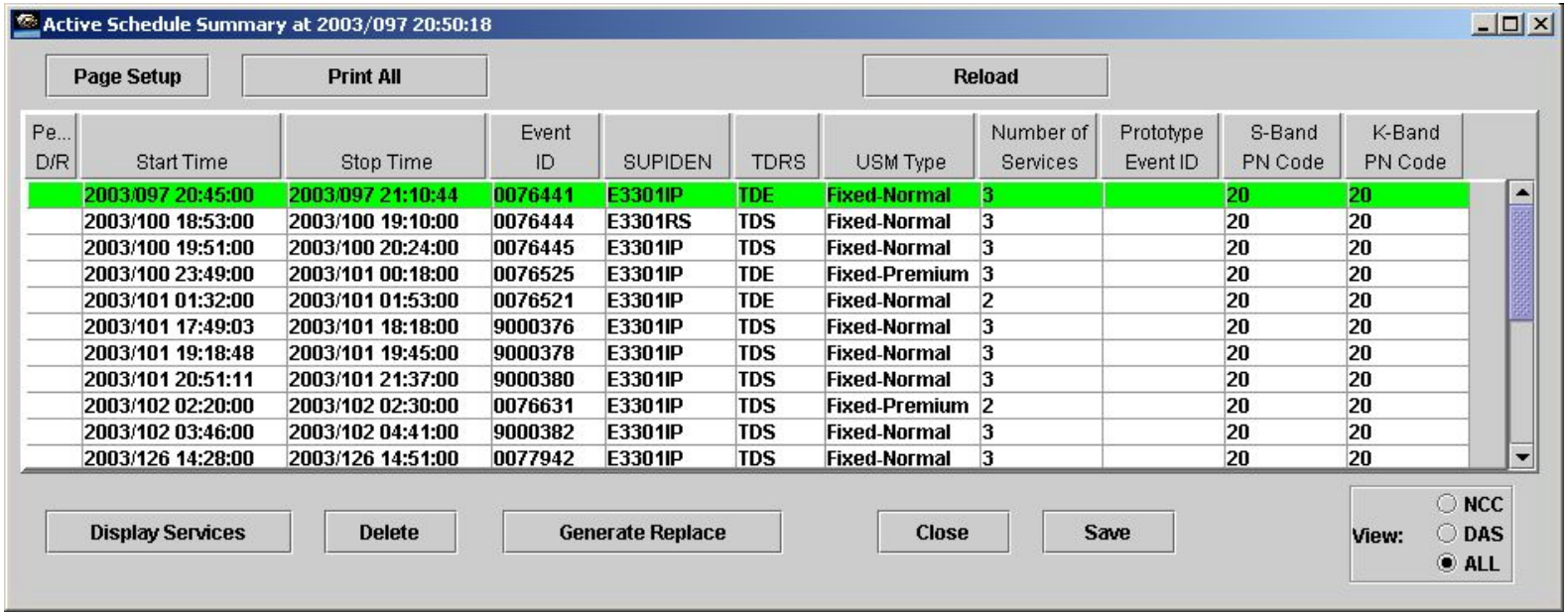


Schedule Requests Summary



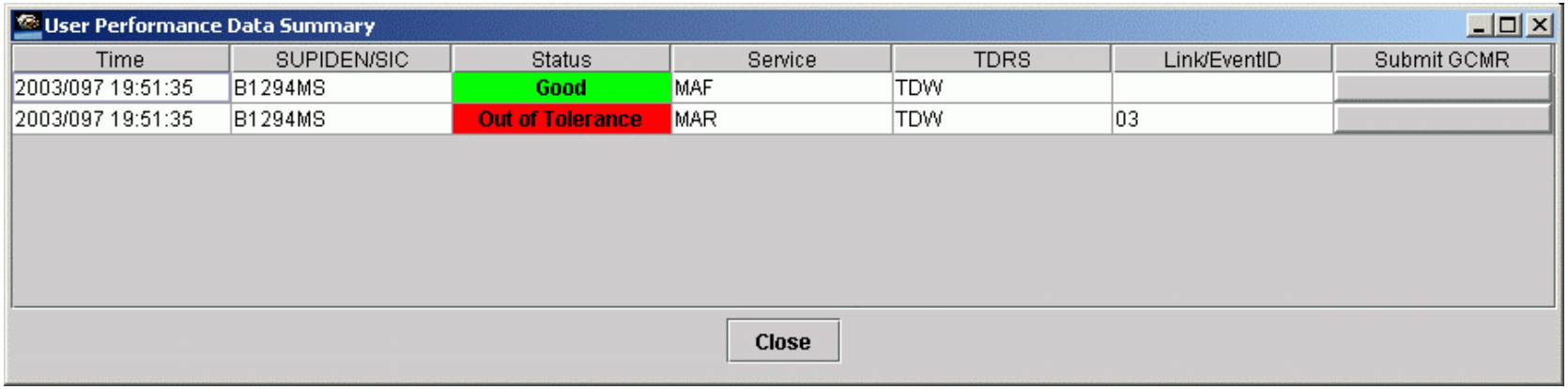
- **History of previously submitted requests**
- **Number of requests displayed dependent on Schedule Request purge time for the SIC(s)**

Active Schedule Summary



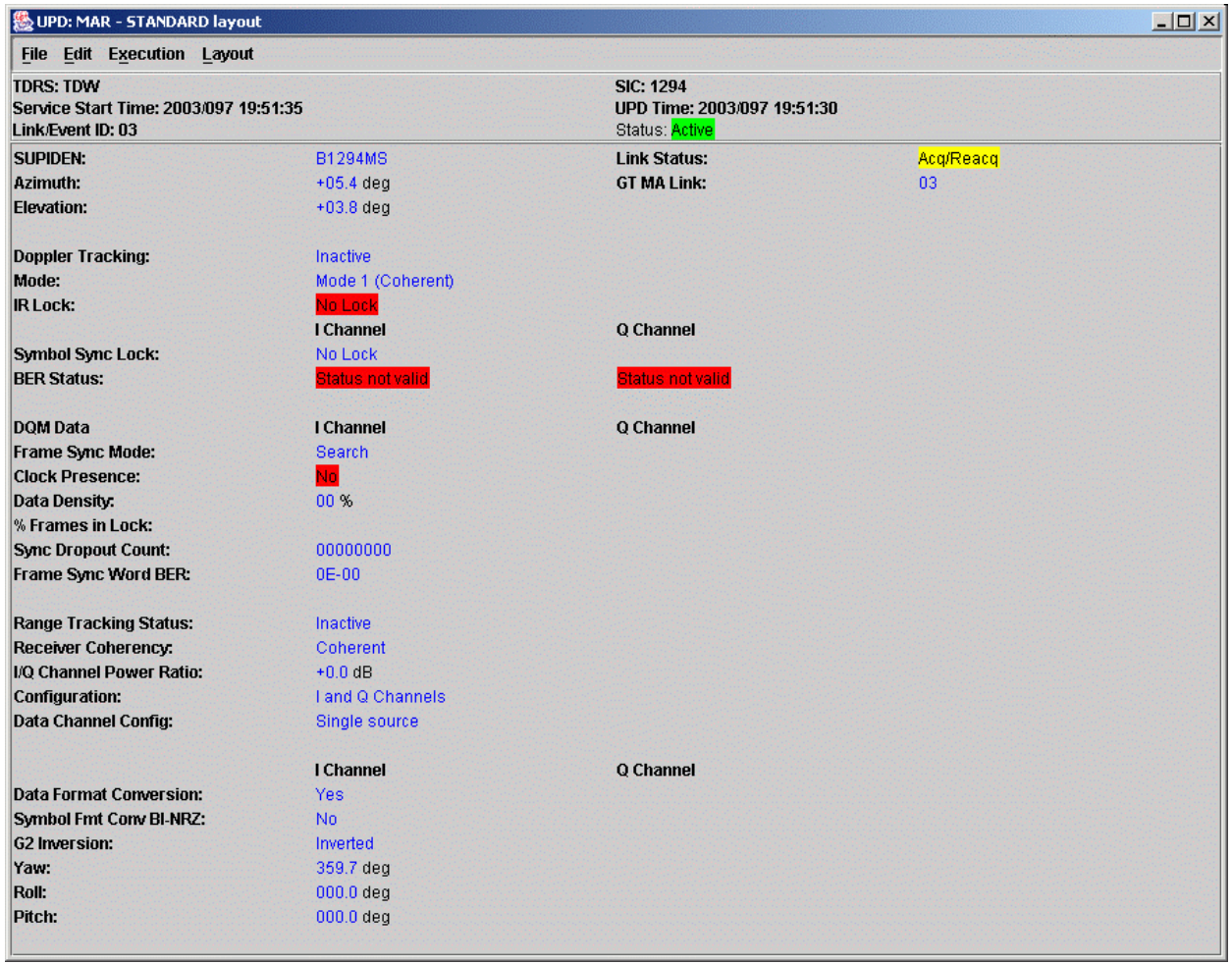
- **Confirmed events for which SWSI has received USM from NCCDS**
- **Only in-progress events or events scheduled to occur in the future**

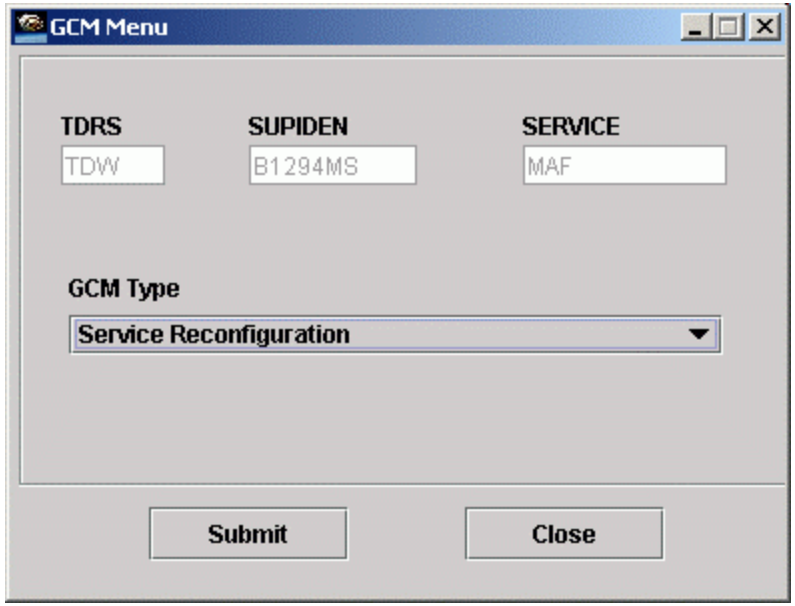
UPD Summary



- **Dynamically updated list of UPD "streams" being received by SWSI for all authorized SICs**
- **UPD Enable not required by user. SWSI always automatically enables UPDs and sends them to the Client application.**
- **Status values based on parameter limit checking, similar to those in CCS UPD displays**

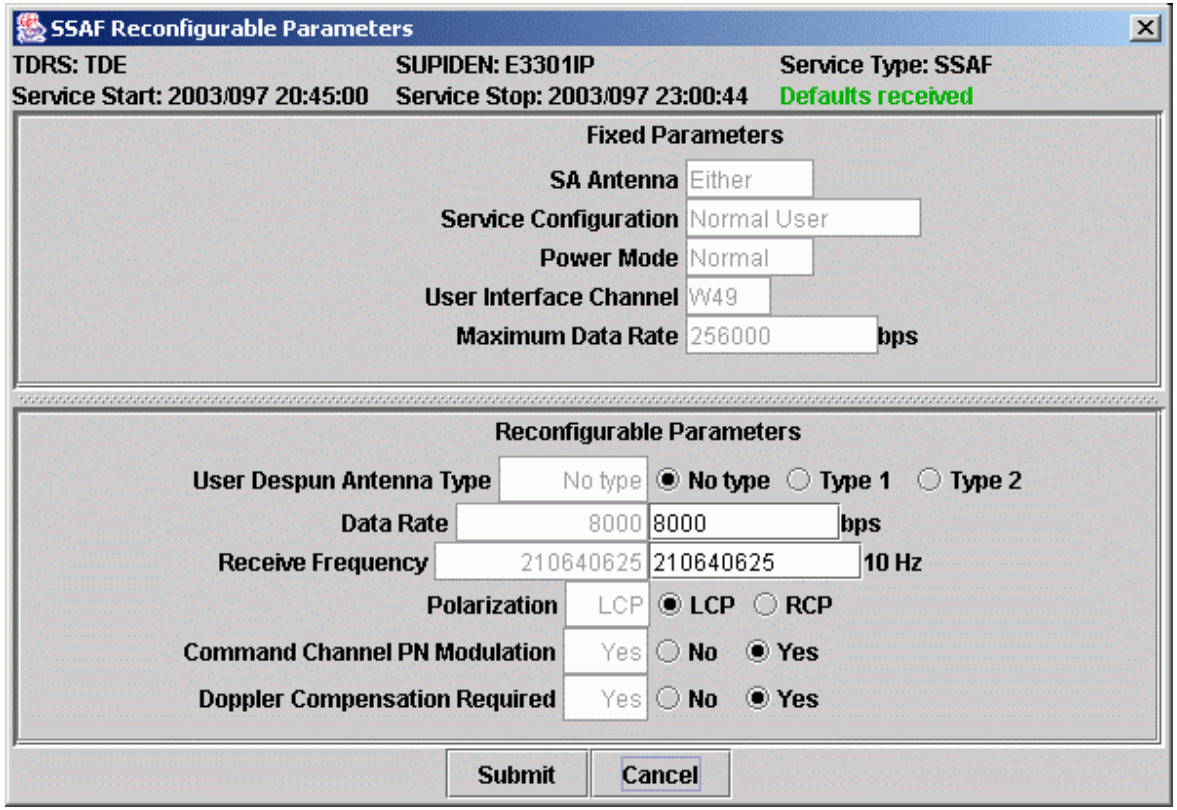
UPD Details


UPD: MAR - STANDARD layout
File Edit Execution Layout
TDRS: TDW
Service Start Time: 2003/097 19:51:35
Link/Event ID: 03
SIC: 1294
UPD Time: 2003/097 19:51:30
Status: Active
SUPIDEN: B1294MS
Azimuth: +05.4 deg
Elevation: +03.8 deg
Link Status: Acq/Reacq
GT MA Link: 03
Doppler Tracking: Inactive
Mode: Mode 1 (Coherent)
IR Lock: No Lock
I Channel
Q Channel
Symbol Sync Lock: No Lock
BER Status: Status not valid
Status not valid
DQM Data
I Channel
Q Channel
Frame Sync Mode: Search
Clock Presence: No
Data Density: 00 %
% Frames in Lock:
Sync Dropout Count: 00000000
Frame Sync Word BER: 0E-00
Range Tracking Status: Inactive
Receiver Coherency: Coherent
I/Q Channel Power Ratio: +0.0 dB
Configuration: I and Q Channels
Data Channel Config: Single source
I Channel
Q Channel
Data Format Conversion: Yes
Symbol Fmt Conv Bi-NRZ: No
G2 Inversion: Inverted
Yaw: 359.7 deg
Roll: 000.0 deg
Pitch: 000.0 deg



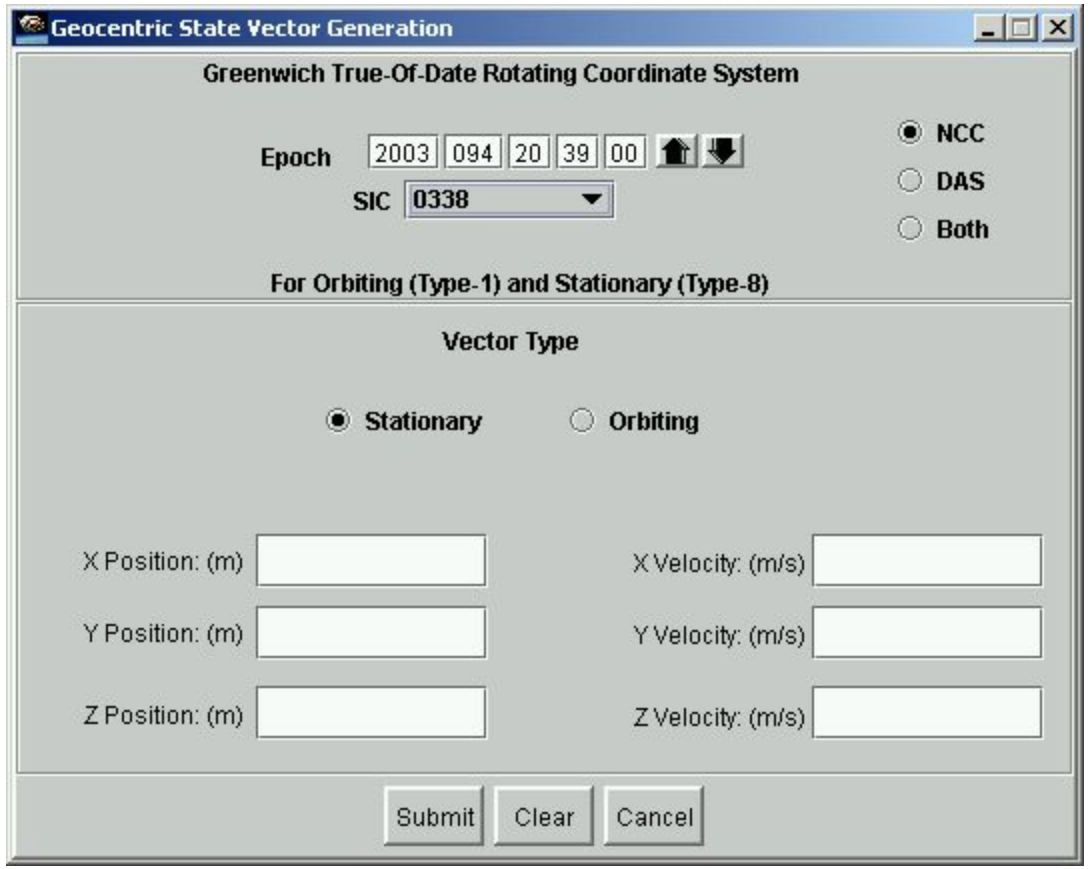
- **Invoked from UPD Summary or Active Schedule Summary panels**

Parameter Reconfiguration

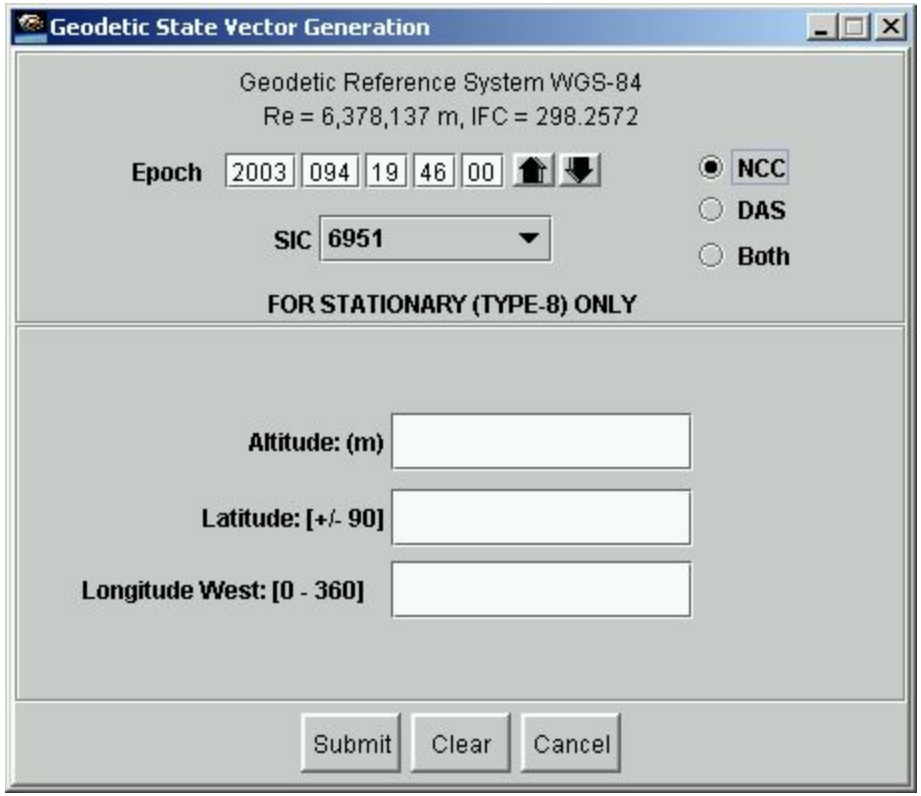


- **Existing parameter values in left column based on initial values from USM plus changes from subsequent GCMRs**

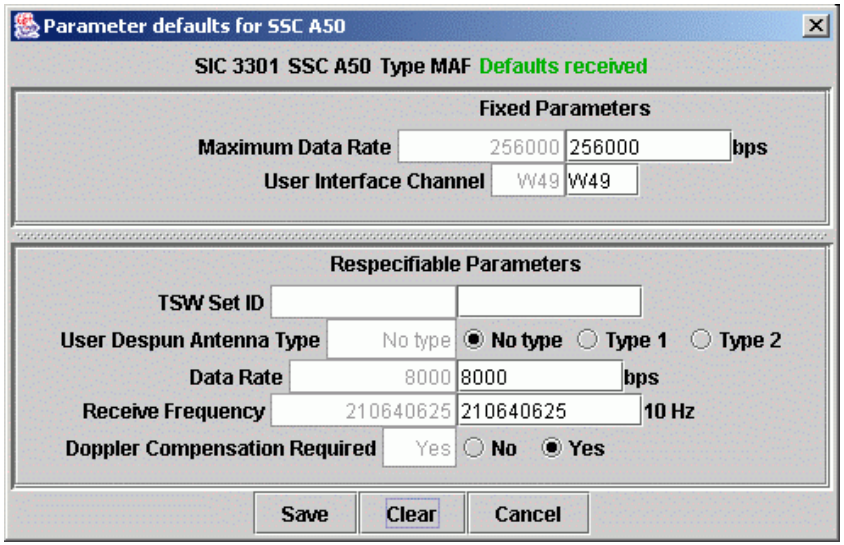
Geocentric State Vector Generation



Geodetic State Vector Generation



SSC Administration



- **NCCDS/SWSI DBA or MOC "Mission Manager" function used to maintain default SSC parameter values**
- **Important for maintenance of DAS parameter values, since the values themselves are sent to DASCON rather than just the SSC code**

Miscellaneous Functions

- **Active Schedule File automatically stored on Client workstation**
- **UPD data logged on Client workstation**
- **Automatic and manual importing of user-formatted State Vector files**
- **Automatic and manual importing of user-formatted TSW files**

Section 3
Server Configuration

Server Hardware
Server COTS/GOTS Software
SWSI Server Applications
Inter-process Communication
HA Configuration
Database Configuration
NISN Secure Gateway Rules

Server Hardware

- **Open Servers**
  - Two Sun Microsystems Ultra 2 desktop workstations
  - 21” color monitor
  - 9 Gbyte internal SCSI disk drive
  - CD-ROM drive
  - External 4 mm 12 Gbyte DDS-3 tape drive
  - Built-in 10/100 Mbps NIC
  - Quad 10/100 Mbps expansion NIC
  - High Availability (HA) configuration using dual heartbeats

Server Hardware (cont'd)

- **Backend Servers**
  - Two Sun Microsystems Blade 1000 desktop workstations
  - 21" color monitor
  - 36 Gbyte internal SCSI disk drive
  - DVD-ROM drive
  - 4 mm 20 Gbyte DDS-4 tape drive
  - Built-in 10/100 Mbps NIC
  - Quad 10/100 Mbps expansion NIC
  - Differential SCSI expansion card for RAID interface
  - High Availability (HA) configuration using dual heartbeats
- **RAID Array**
  - Sun Microsystems 72 Gbyte Storedge A1000 External RAID Array
  - Database storage only

Server COTS Software

- **Sun Solaris 8 Operating System**
- **Java Runtime Environment (JRE) version 1.4.1_02**
  - Executes server Java applications (Application Server, Isolator, etc)
- **Java Development Kit (JDK) version 1.4.1 Java archiver (jar)**
- **Oracle version 8.1.6 (backend servers only)**
- **Oracle JDBC Driver version 9.0.0**
  - Java driver for accessing Oracle
- **Phaos J/CA Toolkit version 1.11-4**
- **Phaos SSLava Toolkit version 1.3**

Server COTS Software (Cont'd)

- **Apache web server 1.3.27**
- **OpenSSL Ben-SSL 1.48**
  - Secure Sockets Library (SSL) extension to Apache web server. Provides encrypted web interface.
- **CohProg SaRL Network Consulting Apache Mod_bandwidth version 2.0.4**
  - Bandwidth limiting extension to Apache web server
- **Sun StorEdge RAID Manager version 6.22 (backend servers only)**
- **TCPWrappers version 7.6**
- **IPFilter version 3.4.31**
  - Firewall to control access by external hosts to specific servers (e.g., HTTPS, Application Server)
- **wget version 1.8.2**

Server GOTS Software

- **High Availability (HA) Application**
  - Controls execution of critical server processes
  - Ensures that only one server in an HA pair is executing the processes at any one time
  - Developed as part of NCC98 for Sun Microsystems platforms (NPG, Firewall, TUT Server
- **HA Graphical User Interface (GUI)**
  - Used to monitor status of HA application
- **NCCDS Protocol Gateway Delogger**
  - Used to view SNIF logs in real time
  - Developed as part of NPG system for NCC98

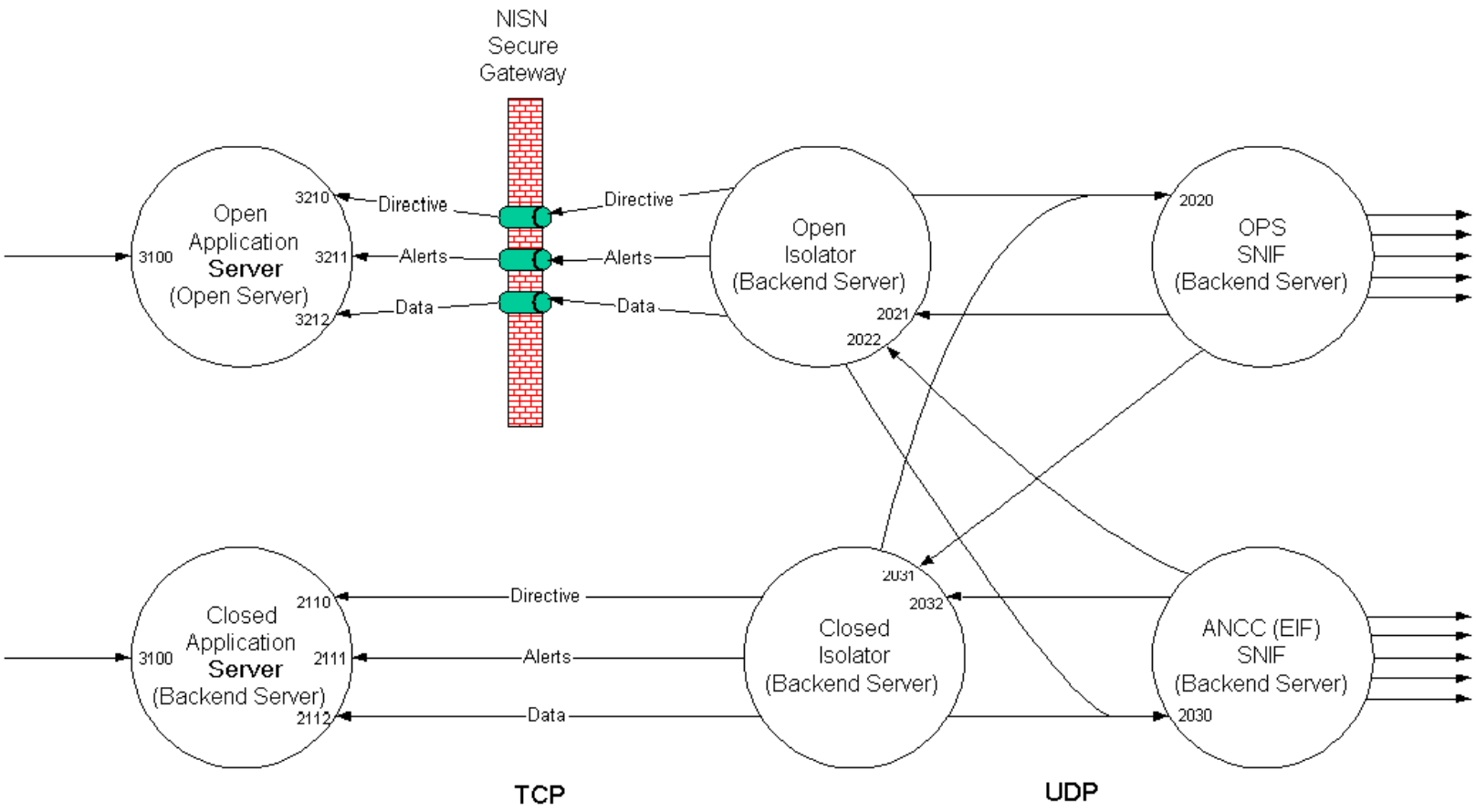
SWSI Server Applications

- **Application Server**
  - Executed under HA control
- **Isolator (Backend Server only)**
  - Executed under HA control
- **SNIF (Backend Server only)**
  - Executed under HA control
- **SDIF (Backend Server only)**
  - Executed under HA control
  - Not provided in initial SWSI release
- **TUT Proxy Sender (Backend Server only)**
  - Executed under cron control
  - Periodically retrieves TUT data files from NCCDS and ANCC TUT servers and forwards them to SWSI open servers
  - Receives user-generated digital certificates from open servers for archival on backend servers

SWSI Server Applications (Cont'd)

- **TUT Proxy Receiver (Open Server only)**
  - Started at system boot time
  - Receives and stores TUT data files transmitted by TUT Proxy Sender from backend server
  - Sends user-generated digital certificates to backend server for archival
- **SWSI Web Page**
  - User digital certificate generation forms and tool
  - SWSI Client software for users to download
- **TUT Web Page (Open Server only)**
  - Mirror of TUT web page provided by NCC
  - Allows users to access TUT via Internet and Open IONet
- **Certificate Generator**
  - Accessed by user via SWSI web page
  - Generates digital certificates for SWSI Client users, SWSI server processes, and SWSI Certificate Authority (CA)

Inter-process Communication



Inter-process Communication (Cont'd)

- **Client-Application Server TCP Connection**
  - Single TCP port to which Client connects
  - Application Server *clientServerConnectionPort* property
- **Application Server-Isolator TCP Connections**
  - Directive Port
    - Directives or requests sent by Clients and forwarded by Application Server to Isolator
  - Events (Alerts) Port
    - Alerts and User Performance Data UPD generated or forwarded by the Isolator to the Application Server
  - Data Port
    - Responses to directives or other data, such as Time Transfer Messages (TTMs), generated or forwarded by the Isolator to the Application Server
  - Isolator *SWSIserverName* and *SWSIserverPort* (base port) properties
  - Application Server *isolatorServerDirectivePort*, *isolatorServerEventsPort*, and *isolatorServerDataPort* properties

Inter-process Communication (Cont'd)

- **Isolator-SNIF UDP Channels**
  - Communication using connectionless UDP protocol
  - Isolator *SNIFhostName*, *SNIFnormPortNumber*, *SNIFnormInPortNumber*, *SNIFeifPortNumber*, and *SNIFeifInPortNumber* properties
  - SNIF *IsolatorReadHost*, *IsolatorReadPort*, *Isolator1WriteHost*, *Isolator1WritePort*, *Isolator2WriteHost*, and *Isolator2WritePort* properties
- **SNIF-NCCDS TCP Connections**
  - TCP/XDR connections with NCCDS or ANCC as defined in *NCCDS/MOC ICD*
  - Separate set of connections maintained on behalf of each SWSI customer SIC

HA Configuration

- **HA application run in background as user *root*, started at system boot time**
- **IP Addressing**
  - Permanent address is always maintained
  - Virtual address floats with Primary workstation
- **Connection to permanent address**
  - TUT Proxy Sender on Backend Server to TUT Proxy Receiver on Open Servers
- **Connection to virtual address**
  - Client application to Application Server
  - Web server
  - Open Isolator on Backend Server to Application Server on Open Server

Database Configuration

- **Four SWSI database instances (OPS, EIF, OPS2, EIF2)**
  - Allows for two different software releases to execute at one time, allow a gradual transition for major releases
  - Initial delivery uses OPS2, EIF2

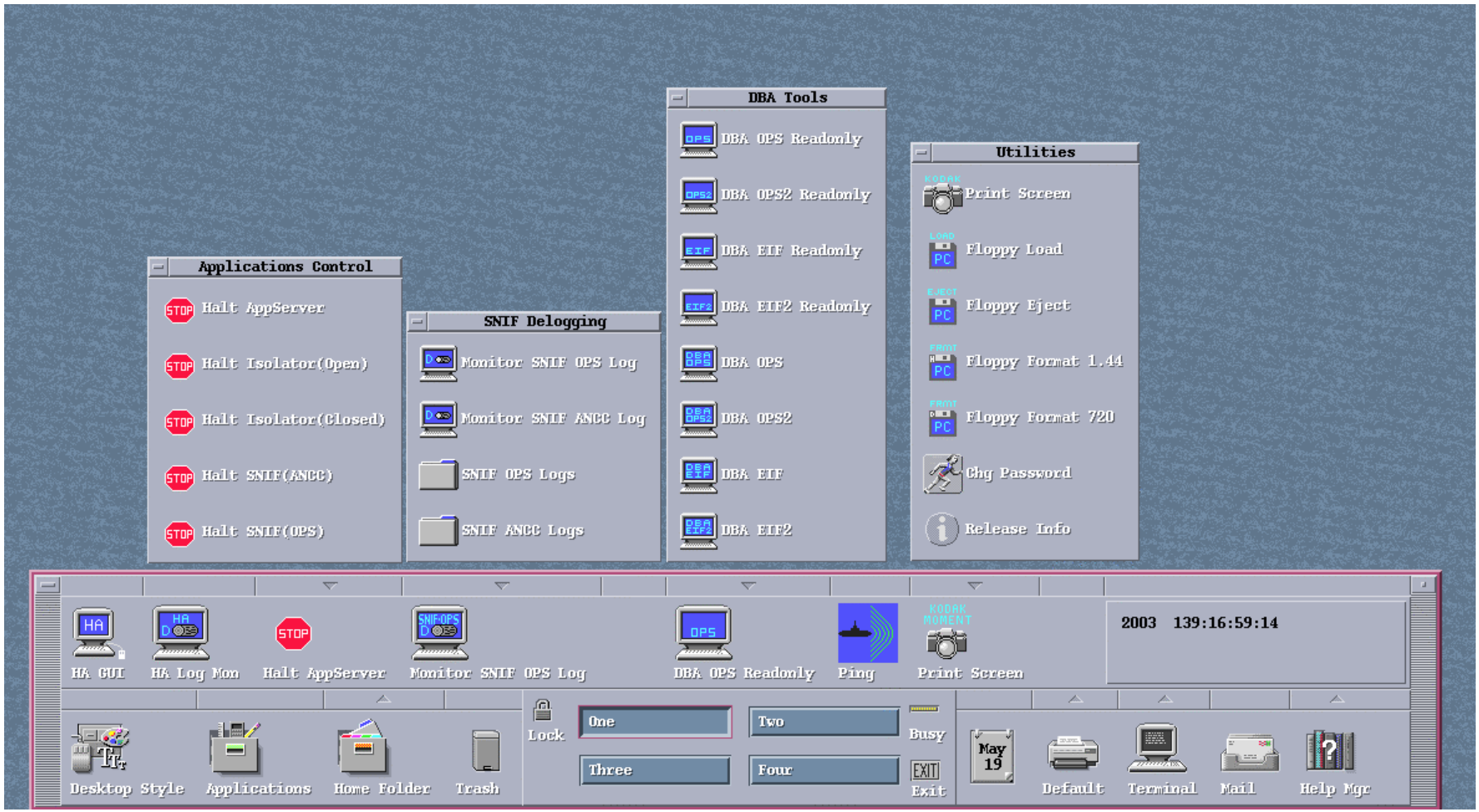
NISN Secure Gateway Rules

Closed IONet Source IP	Open IONet Destination IP	Open IONet Destination TCP Port
Backend Server A Permanent Address	Open Server Virtual Address	Application Server Directive Port (*isolatorServerDirectivePort property)*
Backend Server A Permanent Address	Open Server Virtual Address	Application Server Alert Port (*isolatorServerEventsPort property)*
Backend Server A Permanent Address	Open Server Virtual Address	Application Server Data Port (*isolatorServerDataPort property)*
Backend Server B Permanent Address	Open Server Virtual Address	Application Server Directive Port (*isolatorServerDirectivePort property)*
Backend Server B Permanent Address	Open Server Virtual Address	Application Server Alert Port (*isolatorServerEventsPort property)*
Backend Server B Permanent Address	Open Server Virtual Address	Application Server Data Port (*isolatorServerDataPort property)*
Backend Server A Permanent Address	Open Server A Permanent Address	TUT Proxy Receiver Port (*ServerPort property)*
Backend Server A Permanent Address	Open Server B Permanent Address	TUT Proxy Receiver Port (*ServerPort property)*
Backend Server B Permanent Address	Open Server A Permanent Address	TUT Proxy Receiver Port *(ServerPort property)*
Backend Server B Permanent Address	Open Server B Permanent Address	TUT Proxy Receiver Port *(ServerPort property)*

Section 4
Server Operation

Backend Server CDE Toolbar & Menus
Open Server CDE Toolbar & Menus
DBA Tool Status Monitoring
SNIF Log Monitoring

Backend Server CDE Toolbar



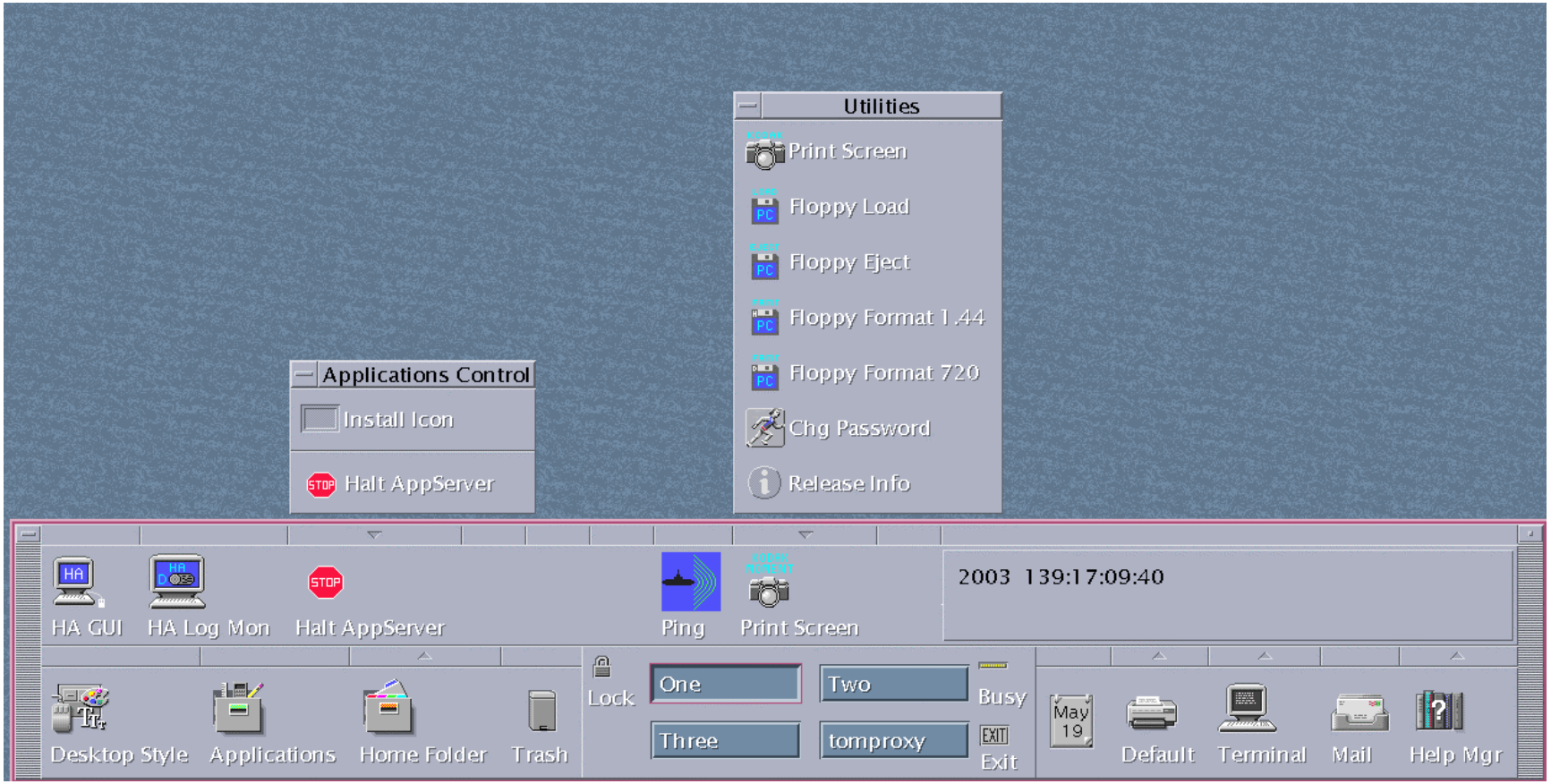
Backend Server CDE Menus

- **HA GUI Button**
  - Monitoring and Control of HA Application
  - Role changes slow because of RAID and Oracle startup and shutdown
  - PRIMARY to HALTED
    - 1-2 minutes
    - No progress indication on main HA GUI panel until status shows HALTED
  - BACKUP to PRIMARY
    - Status shown immediately as PRIMARY, but transition takes 2-3 minutes to complete
    - One cycle of application failures may occur
    - HA Log may be used to monitor progress
- **HA Log Mon Button**
  - Displays HA log file using NPG Delogger
- **Applications Control Menu**
  - Buttons for halting individual SWSI Server applications after configuration or database change. Applications are subsequently restarted automatically by HA Application. These buttons work only for the server which is currently primary.

Backend Server CDE Menus (Cont'd)

- **SNIF Delogging Menu**
  - Displays SNIF log files using NPG Delogger
  - Folder browser buttons point to log file archive directories
- **DBA Tools Menu**
  - SWSI Database Administration Tool
  - *DBA OPS*, *DBA OPS2*, *DBA EIF*, and *DBA EIF2* buttons used by Database Administrator with Oracle account with full update privilege. Oracle username and password entry required.
  - *Readonly* buttons allow system operator to view customer and configuration data, system status. Oracle username and password entry not required.

Open Server CDE Toolbar



Open Server CDE Menus

- **HA GUI Button**
  - Monitoring and Control of HA Application
  - Unlike backend servers, role changes are quick
- **HA Log Mon Button**
  - Displays HA log file using NPG Delogger
- **Applications Control Menu**
  - Buttons for halting Application Server after configuration change. Application Server subsequently restarted automatically by HA Application. These buttons work only for the server which is currently primary.

DBA Tool Status Monitoring

- **Display user activity log**

```
SWSI User Activity Log, EIF database instance
Mon May  5 18:55:39 GMT 2003
------------------------------------------------------------

Time            User ID         Action              IP Address
-------------------------------------------------------------------------------
04/10 21:25:55  sardella        Login               xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
04/10 21:34:09  sardella        Logout              xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
04/11 21:19:49  sardella        Login               xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
04/11 21:37:59  sardella        Logout              xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
04/17 19:02:10  sardella        Login failed        xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
04/17 19:02:40  sardella        Login               xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
04/17 19:09:14  sardella        Logout              xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
05/05 18:49:51  sardella        Logout              xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
05/05 18:53:53  sardella        Passwd chg request  xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
05/05 18:54:03  sardella        Passwd changed      xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
05/05 18:54:03  sardella        Login               xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
05/05 18:54:42  sardella        Logout              xxx.xxx.xxx.xxx (abc.gsfc.nasa.gov)
```

DBA Tool Status Monitoring (Cont'd)

- **Display users logged in**

```
SWSI Users Logged In, EIF database instance
Mon May  5 17:10:54 GMT 2003
-------------------------------------------------------------

User ID              Login Date           IP Address
Server ID            Logout Date          Failed Attempts
-------------------------------------------------------------------------------
sardella             2003/04/28 20:28:03  xxx.xxx.xxx.xxx (xyz.gsfc.nasa.gov)
open                 2003/04/28 20:20:22  0

stevens              2003/04/28 20:21:33  yyy.yyy.yyy.yyy (abc.nascom.nasa.gov)
closed               2003/04/28 20:20:51  0
```

- **Monitor NCCDS connection status**

```
SWSI Connection Status, EIF database instance
Tue May  6 00:22:07 GMT 2003
-------------------------------------------------------------

Name                 schReq  schStatus  acqStore  tswStore  reconfig  pmData
-------------------------------------------------------------------------------
GP-B Scheduling              Active
LSAT-4/5 Scheduling

GP-B Realtime                                                 Active    Active
LSAT-4/5 Realtime                                             Active    Active
```

SNIF Log Monitoring

- **Connection-oriented log messages**
  - GP-B Scheduling schStatus connection established to ANCC
  - GP-B Scheduling schStatus connection to ANCC closed
  - Unable to open GP-B Realtime pmData connection
  - Enabling Schedule Status Connection GP-B Scheduling
  - Disabling Schedule Status Connection GP-B Scheduling
  - Cycling GP-B Realtime pmData connection in preparation for upcoming event
- **Errors caused by SWSI Database problem**
  - Error in <unit_name>, Schedule Connection entry not found for SIC: 8603
  - Error in <unit_name>, Realtime Connection entry not found for SIC: 8603
  - Error initializing GP-B Realtime pmData connection, no SICs
  - Error initializing GP-B Realtime pmData connection, no SUPIDENs for SIC 8603
- **Errors caused by NCCDS Database problem**
  - Error processing SRM, error updating status for ID <request_id>
    - SIC is configured for baseline rather than full support
- **Errors caused by NCCDS problem**
  - Error processing UPD ID #<message_id>, <error_condition>

Section 5
Customer and User Setup

Adding Customers
Adding SWSI Client Users
SSC Management
Client User Login Problems

Adding Customers

- **All SWSI customers are full support**
- **Schedule Request purge time**
  - Establish with customer how long after requested event start time to keep Schedule Requests before they are purged from SWSI Database
  - Affects how many requests are displayed in Client Schedule Request Summary panel
  - Purge time entered into SWSI Database along with SIC
- **Spacecraft Identification Code (SIC)**
- **SUPIDENs**
- **Schedule Connection**
  - Establishes configuration for connecting to SPS
  - SIC may be added to existing Schedule Connection entry. SPS must be configured to send schedule results for new SIC to same Logical Destination.
  - For new Schedule Connection entries, NCCDS DBA must create new Logical Destination, User ID, and Password. Information is entered into both NCCDS and SWSI databases and is not shared with customer.

Adding Customers (Cont'd)

- **Realtime Connection**
  - Establishes configuration for connecting to NPG on behalf of CCS
  - SIC may be added to existing Realtime Connection entry. CCS must be configured to send reconfiguration and performance data for the new SIC to the same destination.
  - For new Realtime Connection entries, NCCDS DBA must create new User ID and Password. Information is entered into CCS, NPG, and SWSI databases and is not shared with customer.
- **Prototype Event Codes**
- **Service Specification Codes (SSCs)**
  - Codes added using Server DBA Tool have default parameter values set to NULL. If true default values desired, entry is from SWSI Client by a DBA or Mission Manager.

Adding Customers (Cont'd)

- **Active Schedule Upload**
  - Establish with customer whether they would like to receive an Active Schedule file on connected workstations
  - Poll Period
    - Whether to send a new file when it changes and, if so, how often to check for changes
  - Periodic Frequency
    - Whether to periodically send a new file regardless of whether there are changes and how often
  - Include Parameters
    - Whether to include initial service parameter values
  - Translate Enumerated
    - For enumerated parameter types, whether to send numeric value or an enumerated text string

Adding SWSI Client Users

- **User must read and sign SWSI Client User Rules of Behavior**
- **IP address(es) to connect from for entry into IPFilter firewall**
- **Contact information**
  - Full user name
  - Company
  - Mission name
  - Geographic location
  - Phone number
  - Email address
- **Whether user should be allowed Mission Manager privileges, allowing user to edit initial SSC parameter values**
- **Assign userid (e.g., first initial plus last name) and temporary password. Password should be set to expired to force user to set new password on initial login.**

SSC Management

- **SSC default parameter values only important if user is respecifying parameter values for a SAR, or if user would like to see them for information purposes only when generating requests. When event is scheduled, user will be able to view parameter values extracted from USM.**
- **Parameters can still be respecified if default value is NULL or incorrect. Again, it is there for information purposes only.**
- **Care should be taken when modifying default values to make sure modification is made to both NCCDS Database and SWSI Database.**
- **DAS SSCs are internal to SWSI, so no coordination is required. Customer Mission Manager is responsible for maintaining default parameter values.**

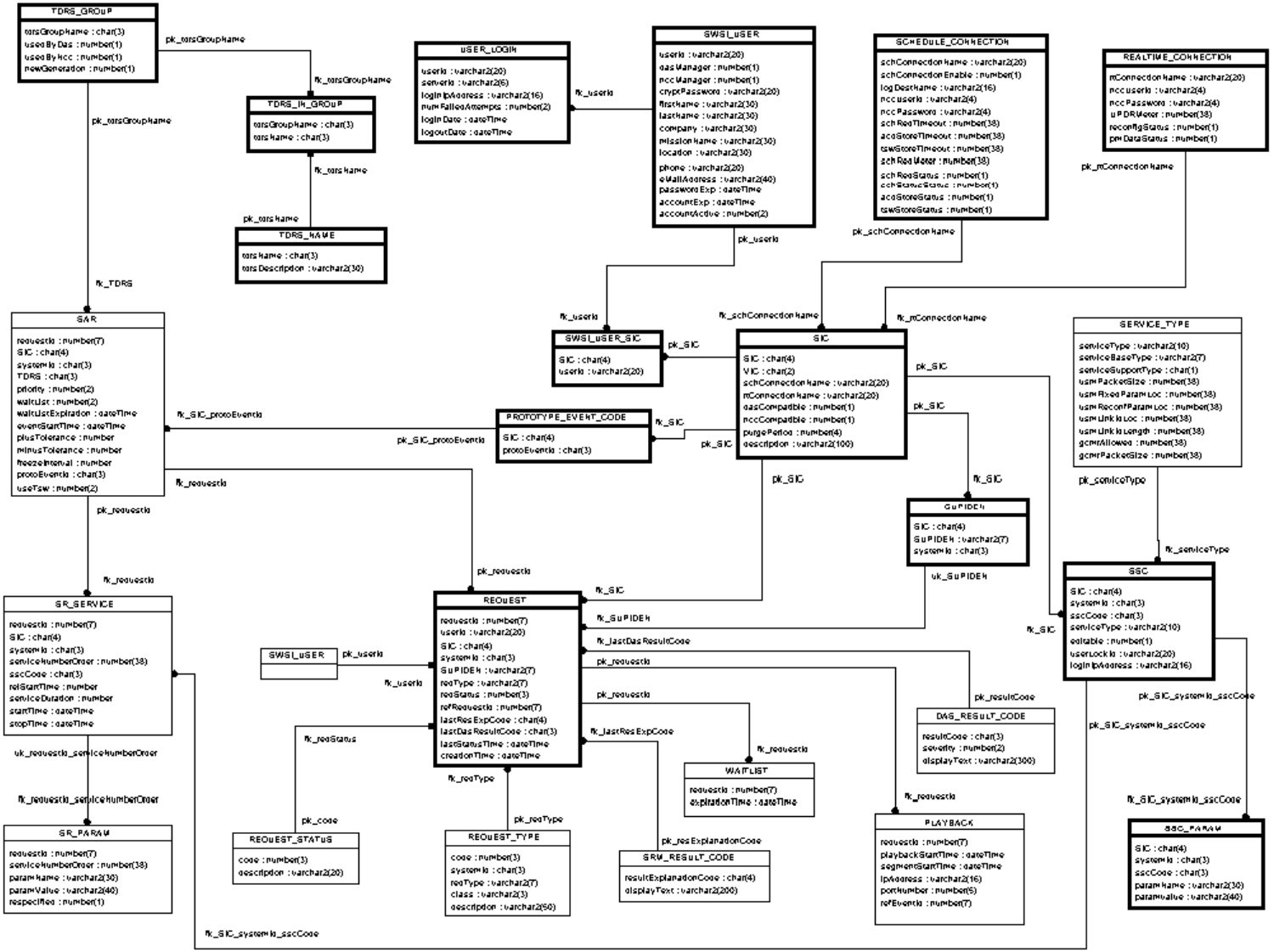
Client User Login Problems

- **Client user may receive error dialog stating that userid or password is invalid, or that the user may already be logged in from same IP address**
- **Troubleshooting procedure**
  - Check that userid exists in SWSI Database
  - Check whether account has been deactivated because of too many failed login attempts, which can happen if a user forgot his password. If so, the SWSI DBA should do the following:
    - Reset password to a temporary value
    - Set password expiration date to 0 (expired)
    - Reactivate account
    - Give temporary password to user. User will be required to change password after a successful login.
  - Check to see if user is already logged in. If so, inform user that he may still have another SWSI Client application running on the same host and connected to the SWSI Server. If this is not the case, then the problem may be caused by a known bug (Bug #520) in the SWSI Server applications. To fix the problem, do one of the following:
    - Use the DBA Tool to mark the user as logged off
    - Restart the appropriate Application Server

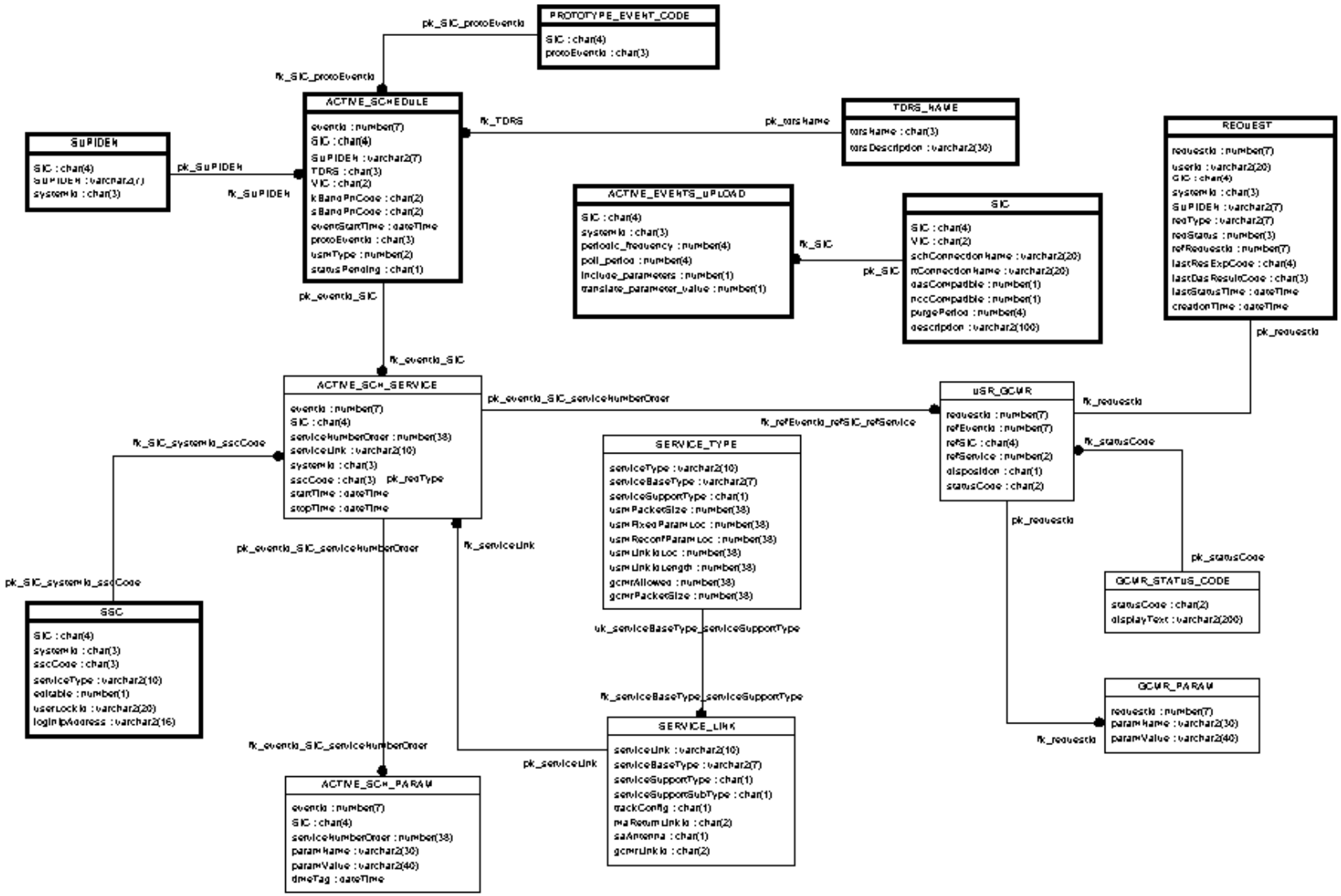
Section 6
Database Design and Management

Database Schema
Database Tables
Oracle Accounts

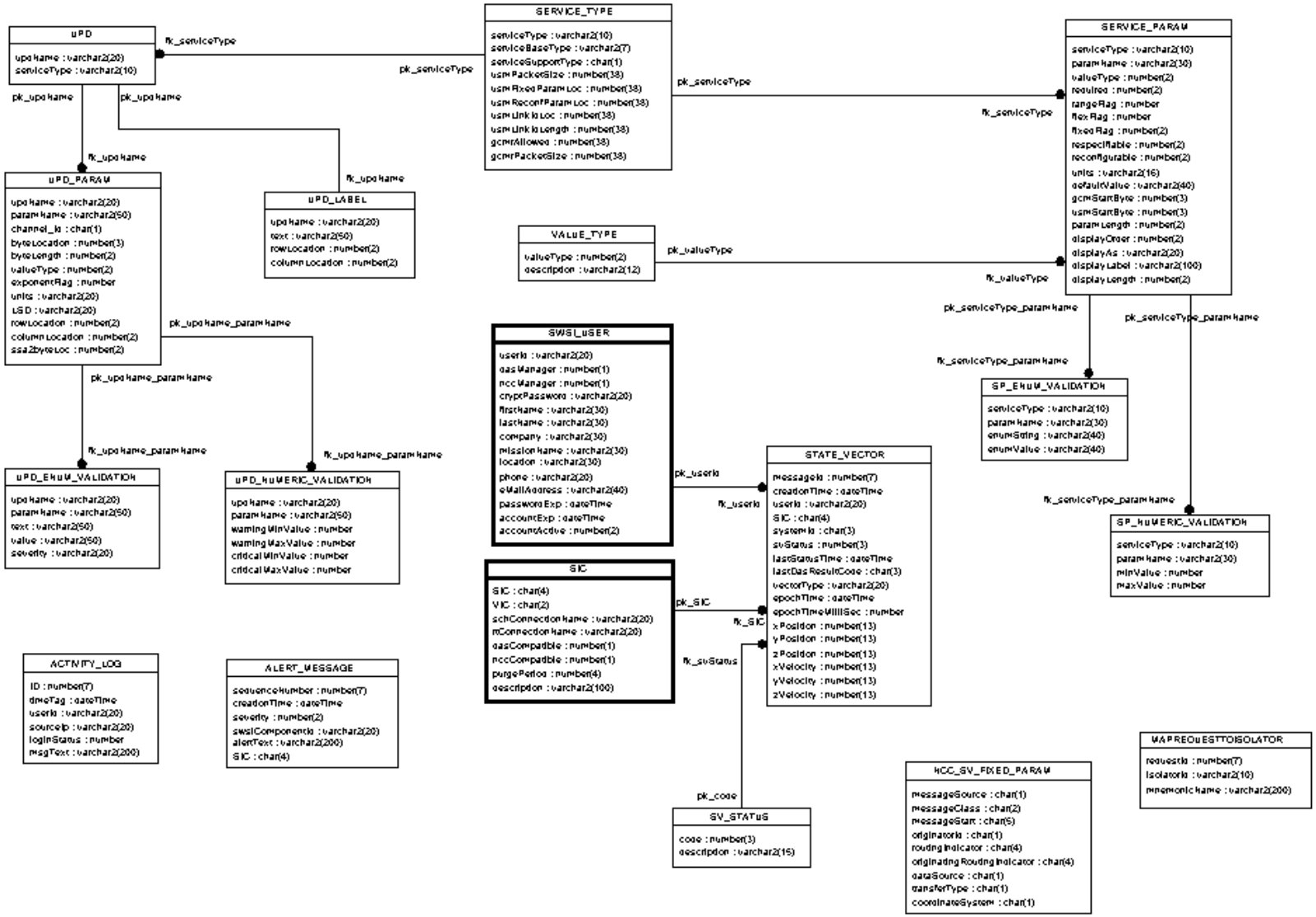
Database Schema (1 of 3)



Database Schema (2 of 3)



Database Schema (3 of 3)



Database Tables

- **ACTIVE_EVENTS_UPLOAD**
  - Parameters for periodic upload of active schedule file(s) to Client workstations
- **ACTIVE_SCHEDULE**
  - Active (confirmed) events, derived from User Schedule Messages (USMs) received from NCCDS
- **ACTIVITY_LOG**
  - Client login/logout events
- **PROTOTYPE_EVENT_CODE**
  - Valid NCCDS Prototype Event Codes assigned to a SIC
- **REALTIME_CONNECTION**
  - NCCDS realtime connection (reconfig, pmData) configuration
- **REQUEST**
  - NCCDS and DAS schedule requests
- **SCHEDULE_CONNECTION**
  - NCCDS scheduling connection (schReq, schStatus, etc.) configuration
- **SIC**
  - Support Identification Codes (SICs) for spacecraft supported by SWSI

Database Tables (Cont'd)

- **SSC**
  - Valid Service Specification Codes (SSCs) assigned to a SIC
- **SSC_PARAM**
  - Default parameter values for an SSC
- **SUPIDEN**
  - Valid Support Identifiers (SUPIDENs) for a SIC
- **SWSI_USER**
  - SWSI Client user information
- **SWSI_USER_SIC**
  - SWSI Client user SIC authorizations
- **TDRS_GROUP**
  - Valid TDRS group/set names
- **TDRS_IN_GROUP**
  - TDRS group/name assignments
- **TDRS_NAME**
  - Valid TDRS names
- **USER_LOGIN**
  - Information about SWSI Client users who are or were logged in

Oracle Accounts

- **SWSIDB**
  - Owns the schema and has full privilege
- **SWSIOPS**
  - Readonly account for SWSI operator access
  - Used for viewing data and system status, but not modify data
- **ORASWSI**
  - Used by SWSI Server applications (Isolator, SNIF, SDIF) to access tables.
  - Username and password entered into property or configuration files for server applications
- **DBA Accounts**
  - Assigned to individual Database Administrators to use with SWSI DBA Tool
  - Update, insert, and delete privilege

Section 7
Database Administration

- **Database Administration Tool**

```
SWSI DBA Version Build 4 Patch 02, EIF database instance
Main Menu

 1 = User Administration
 2 = NCCDS Schedule Connection Administration
 3 = NCCDS Realtime Connection Administration
 4 = SIC Administration
 5 = Prototype Event Code Administration
 6 = SUPIDEN Administration
 7 = TDRS Name Administration
 8 = SSC Administration
 9 = Active Schedule Upload Administration

 q = Quit

Enter command:
```

Database Administration (Cont'd)

- **User Administration**
  - User accounts and SIC authorizations
  - Users logged in
  - Activity log
- **Schedule Connection Administration**
  - Configuration of SNIF connections (scheduling, state vector storage, TSW storage) with SPS
- **Realtime Connection Administration**
  - Configuration of SNIF connections (GCMR, Performance Data) with NPG/CCS
- **SIC Administration**
  - SIC maintenance
  - Manual purging of schedule requests
  - Manual purging of active events
- **Prototype Event Code Administration**
- **SUPIDEN Administration**

Database Administration (Cont'd)

- **SUPIDEN Administration**
- **TDRS Name Administration**
  - Maintenance of TDRS Names and TDRS Set (Group) Ids used by Client in creating Schedule Requests
- **SSC Administration**
  - SSC Code entry (codes only, no default parameter values)
- **Active Schedule Upload Administration**
  - Configuration parameters for upload of Active Schedule file to Client workstations

Section 8
Digital Certificate Management

Digital Certificate Overview
Certificate Authority
Web Server Certificates
Application Server Certificates
SWSI Client User Certificates

Digital Certificate Overview

- **SWSI certificates based on Public Key Infrastructure (PKI) with key pairs**
  - Private Key
    - Used to decrypt or digitally fingerprint (sign) data
    - Kept secret by user
  - Public Key
    - Used to encrypt data or verify signatures (digital fingerprints)
    - Distributed to public
- **Digital Certificate**
  - Contains user's identification with user's public key
  - Contains secure information to verify owner's identity
- **Digital Fingerprint (signature)**
  - Data encrypted with user's private key
  - Provides guarantee to a recipient of the signed data that it has not been modified
  - Verifies source of the signed data

Digital Certificate Overview (Cont'd)

- **Certificate Authority**
  - Creation and management of certificates
- **Registration Authority**
  - Identification, authentication, and registration of certificate subscribers
  - Performs certificate and key management functions on behalf of the CA

Certificate Authority

- **SWSI acts as its own CA and RA**
- **Phaos J/CA toolkit used to generate digital certificates, including CA's public and private keys**
- **SWSI CA configured for 10 year lifetime**
- **Each user and application certificate created is signed with CA's digital fingerprint. Digital fingerprint used in client-server authentication process.**
- **New CA must be generated if it is believed that existing CA has become compromised, such as from a SWSI server intrusion. With new CA, all user and application certificates must be regenerated.**
- **Application Server will operate with two CAs, allowing for overlap during transition from compromised or expired CA to new CA**

Web Server Certificates

- **SWSI acts as its own CA and generates own self-signed certificates for secure web server**
- **OpenSSL used to generate Privacy Enhanced Mail (PEM) certificates for use with Apache web server**
- **SWSI servers delivered with web server certificates configured to expire in 10 years**

Application Server Certificates

- **Application Server digital certificate used for SSL connections with Client application**
- **Phaos J/CA toolkit used to generate Application Server certificate**
- **SWSI servers delivered with Application Server certificate configured to expire in 10 years**

SWSI Client User Certificates

- **Each SWSI Client user generates their own unique digital certificate using web-based generation tool**
- **User certificates expire 366 days after creation**
- **Certificates remain available for download by the user for 30 minutes**
- **Certificates generated on open servers transferred via TUT Proxy to SWSI backend servers for permanent archival**

Section 9
System Administration Procedures

Backup and Recovery
IPFilter Configuration
Background Procedures

Backup and Recovery

- **Full backups of internal workstation disks performed after major system change (software delivery, etc)**
- **Database backups on RAID performed incrementally on a daily basis by automated script**
  - Database backup stored on internal disk on backend server, then copied to tape

IPFilter Configuration

- **Firewall services control access to secure web server (HTTPS) and Client/Application Server ports**
- **Client user IP addresses must be entered by SysAdmin into appropriate (backend or open server) IPFilter table**
- **All entries must be added to both primary and secondary servers**
- **ipfconfig script used to manage table**
- **Adding an IP address**

```
ipfconfig -a 192.168.1.3 "Mission Alpha, John Doe, 555-876-5309,
   john.doe@toetag.com"
```

- **Removing an IP address**

```
ipfconfig -r 192.168.1.3
```

- **Listing all IP addresses**

```
ipfconfig -l
```

- **Interactive mode allows editing other than two standard ports**

```
ipfconfig -I
```

Background Procedures

- **root cron jobs**
  - db2tape.sh
    - Run daily only on backend server to write database backup files to tape
  - ntpdate
    - Run hourly on all servers to update system time
- **swsiops cron jobs**
  - SendTut.csh
    - Run hourly only on backend server to send TUT data to both open servers
  - clean_tut_temp
    - Run daily only on open servers to remove temporary TUT web server files
  - purge_databases
    - Run daily only on backend servers to purge old Schedule Requests and Active Events from all four SWSI database instances

Section 10
Problem Reporting and Tracking

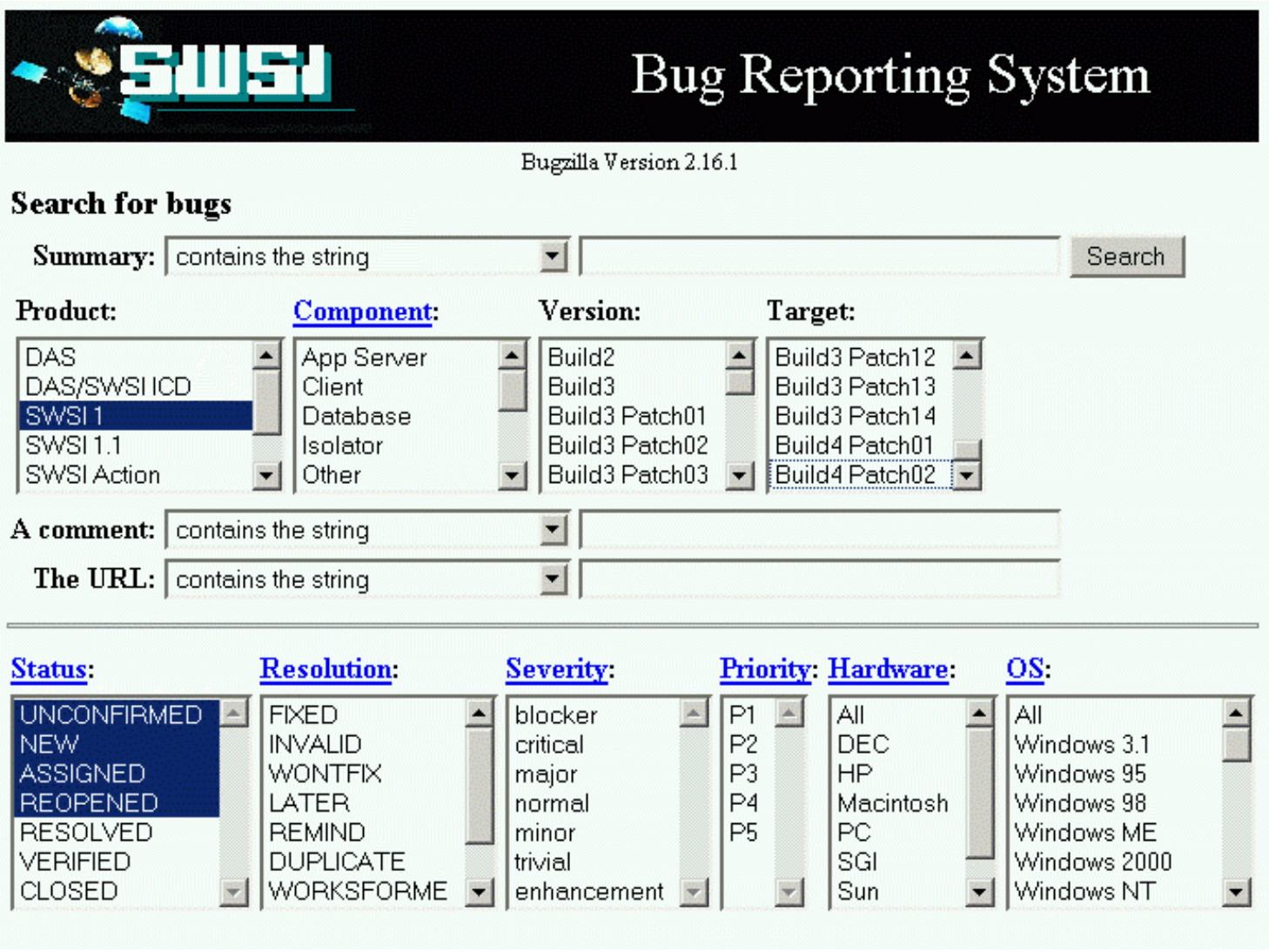
Bugzilla
Bug Writing Guidelines
Known Bugs and Workarounds

Bugzilla

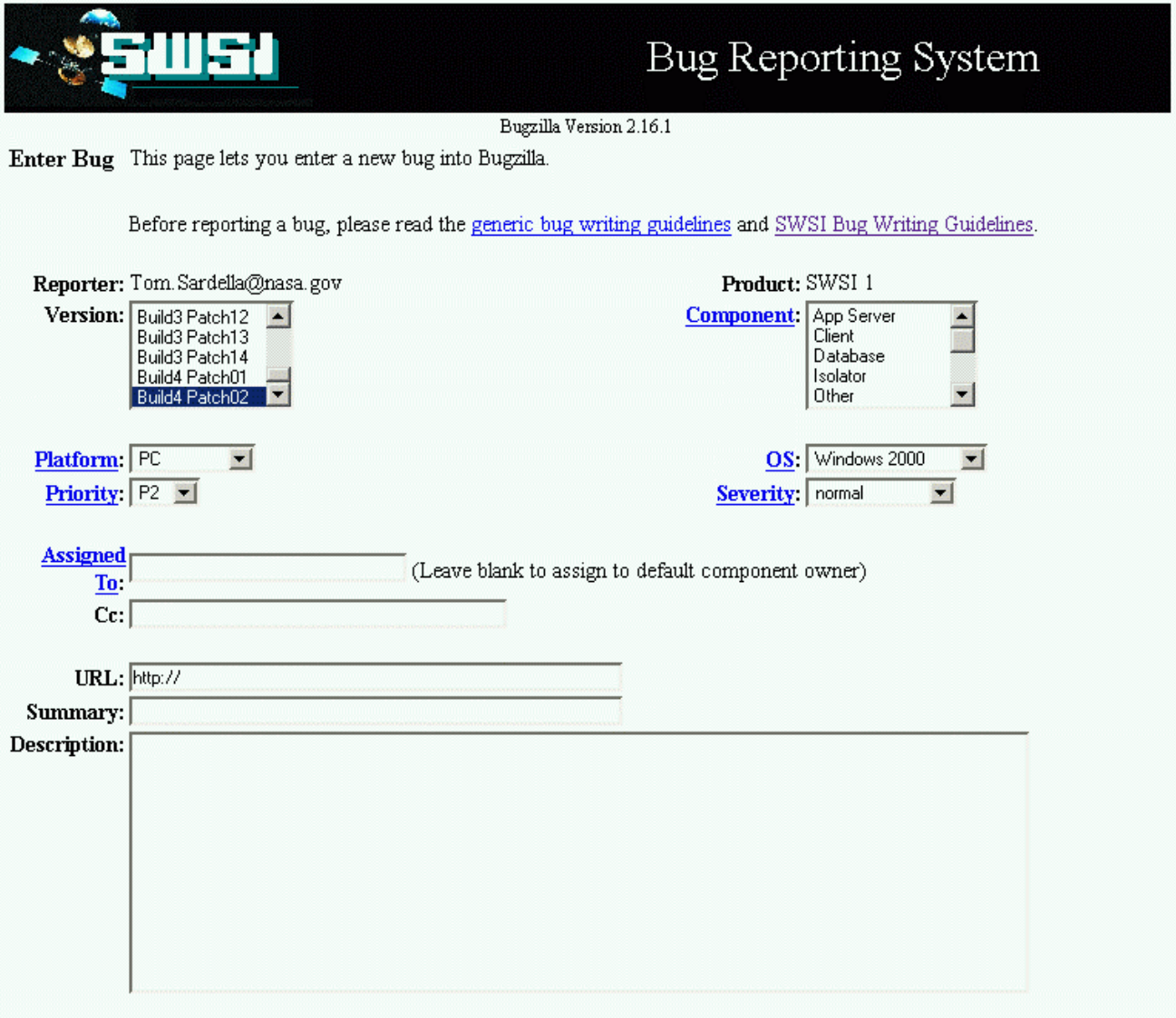
- **Bugzilla is an open source web-based problem tracking system**
  - http://www.bugzilla.org/
- **Accessible through SWSI web page**
  - http://swsi.gsfc.nasa.gov/
  - http://swsi.gsfc.nasa.gov/bugzilla/
- **Account may be applied for online**
- **Web form for building ad-hoc and preset queries**
- **Email notification of updates to existing bugs**
- **Used by SWSI not just for bugs**
  - Enhancement requests from customers
  - System Administration issues
  - Documentation (ICD, Users Guide) issues
  - Action Items

Applying for a Bugzilla Account

Querying Bugzilla (Open Bugs)



Creating a Bug



Bug Writing Guidelines

- **Is there already an open bug for the problem?**
- **One problem/bug. Split multiple problems into several bugs for easier tracking.**
- **Provide plenty of details**
  - Time of occurrence
  - Server(s) that problem occurred on (open or closed, and which server was prime)
  - Which NCCDS (OPS or ANCC)?
  - What customer or user experienced the problem?
  - ID numbers of SARs, etc
  - Exact alert message or error dialog text
  - Is bug reproducible?
- **What other details? Provide screen snapshots as attachments, if available.**

Known Bugs and Workarounds

- **Bug #520, Users sometimes not logged off properly**
  - Bug is RESOLVED WORKSFORME, but not sure if completely fixed
  - Symptom is that user can't log in because server says that user is already logged in from that IP address
  - Workaround is to restart appropriate Application Server. Other connected users will be disconnected, then automatically reconnected.
- **Bug # 556, UPDs not received for overlapping support on multiple TDRSs**
  - Shuttle only known SN customer requiring overlapping support
  - Possible workaround is to use different SUPIDEN with each event
- **Bug #894, NULL Link ID for Track services in Active Schedule File**
  - Was issue for Landsat-7, but they've developed a workaround
- **Bug #896, DBA Tool Rejects Password with Certain Characters**
  - Can't use "*" or "=", maybe some others
- **Bug #904, Users unable to login**
  - Restart Isolator

Section 11
Troubleshooting Procedures

Troubleshooting Procedures

- **During initial setup, user is unable to connect to server**
  - Use network monitoring tool to determine if TCP connection is being attempted
  - If no TCP handshake, probably a network problem at user facility
  - If TCP handshake attempted but not completed, possibly an IPFilter configuration problem
- **User reports no UPD, possibly because CCS thinks the site is "down" (Bug #385)**
  - SNIF cycles pmData connection five minutes before event start time to force a UPD Enable, so problem should rarely occur
  - Site must be brought back manually up from CCS display
- **User reports no UPD, but CCS is transmitting**
  - UPD may not be properly formatted
  - Verify UPD receipt by viewing SNIF log, which will also indicate formatting errors

Troubleshooting Procedures (Cont'd)

- **Client user may report Yellow or Red alert condition**
  - Client Users Guide Appendix A explains what to do for specific alerts
  - Some problems indicate software errors that need to be reported to developers
  - SNIF-related alerts can be examined in more detail by viewing SNIF log
  - SWSI Database problems
    - Schedule and Realtime Connection configuration
    - Missing SSC (error storing USM)
  - NCCDS Database problems
    - SIC configured for baseline rather than full support (dropped SRMs)
  - NCCDS connection problems
    - User receives alert if unable to connect for message transmissions (Schedule Requests, State Vectors, TSWs, GCMR)
- **SWSI Client may be used to monitor server process status**